# Politique d'usage des analytics vidéo

| Référence | Version | Date | Catégorie |
|---|---|---|---|
| **POL-VMS-003** | v1.2 | Mai 2025 | Exploitation VMS & Vidéosurveillance |

Les fonctions d'analyse vidéo intelligente (analytics) enrichissent les systèmes de vidéoprotection de capacités de détection et d'alerte automatisées. Leur déploiement doit cependant respecter un cadre juridique strict et faire l'objet d'une évaluation préalable au regard des finalités poursuivies et des risques pour les droits et libertés des personnes. Cette politique définit les analytics autorisés, ceux soumis à évaluation renforcée et les conditions minimales de déploiement.

---

## 01. Analytics autorisés sans évaluation renforcée

Les analytics suivants peuvent être déployés sans évaluation juridique préalable spécifique, sous réserve que leur finalité soit exclusivement sécuritaire et qu'ils ne génèrent pas de données personnelles identifiantes : détection de mouvement, détection d'intrusion dans une zone prédéfinie, comptage anonymisé de personnes, détection d'abandon de colis ou d'objet suspect, franchissement de ligne virtuelle.

Ces analytics sont considérés comme des outils d'aide à la surveillance, générant des alertes que l'opérateur humain doit valider avant toute action. Ils ne sauraient en aucun cas se substituer à la vigilance humaine ni déclencher automatiquement des mesures affectant des personnes.

---

## 02. Analytics soumis à évaluation juridique

Les analytics suivants nécessitent une évaluation juridique formelle, incluant a minima une Analyse d'Impact relative à la Protection des

Données (AIPD/DPIA) avant tout déploiement : analyse comportementale (détection de comportements jugés anormaux ou suspects), suivi de trajectoires individuelles, estimation démographique (âge, genre), analyse d'affect ou d'état émotionnel.

La reconnaissance faciale, la lecture automatique de plaques d'immatriculation (LAPI) et tout analytics croisant les données vidéo avec d'autres bases de données font l'objet de politiques dédiées et ne sont pas couverts par la présente politique générale.

Le déploiement de tout analytics soumis à évaluation est conditionné à l'accord écrit du DPO de l'organisation cliente, à l'issue d'une procédure de validation d'une durée minimum de 30 jours. Mileo Technology accompagne ses clients dans la réalisation de l'AIPD.

---

## 03. Supervision humaine obligatoire

Quelle que soit la catégorie de l'analytics déployé, la supervision humaine des alertes générées est obligatoire. Aucun système de vidéoprotection équipé d'analytics ne peut fonctionner en mode entièrement automatique, sans qu'un opérateur humain soit en mesure de valider ou d'infirmer les alertes dans un délai raisonnable.

Les opérateurs chargés de la supervision des alertes analytics doivent recevoir une formation spécifique portant sur le fonctionnement du module, les typologies de faux positifs les plus fréquents et les procédures de validation et d'escalade. Cette formation est dispensée par Mileo Technology lors de la mise en service du système.

---

## 04. Validation et révision des paramètres

Les paramètres de sensibilité des analytics (seuils de déclenchement, zones de détection, plages horaires d'activation) sont définis lors de la mise en service et consignés dans la documentation technique du système. Toute modification de ces paramètres suit la procédure d'administration VMS et est soumise à validation du Responsable Sécurité.

> **Une revue semestrielle des performances des analytics déployés est réalisée conjointement par Mileo Technology et le Responsable Sécurité. Cette revue analyse les taux de faux positifs et de faux négatifs, évalue la pertinence des zones et des seuils configurés et formule des recommandations d'ajustement.**


*Boulevard de Courcelles, 75008 Paris — hello@mileotech.com*